

Amendment to the Claims:

This listing of claims replaces all prior versions, and listings, of claims in the application:

1. (previously presented) A method of managing a network session comprising:

delivering security policies from a server to a remote system that has predetermined configuration information and allows running at least one application program;

establishing a secure virtual private network connection between the server and the system; and

regulating activities in the system based on both of the security policies and a context of said at least one application program including at least a state of running of said at least one application program.

2. (previously presented) The method of claim 1 wherein said regulating the activities comprises providing filters that are adapted to reject unauthorized data packets based on rejection criteria that are conditioned on said running state.

3. (previously presented) The method of claim 2 wherein the rejection criteria include the predetermined configuration information.

4-5. Cancelled

6. (Original) The method of claim 1 wherein regulating the activities comprises:

providing a session layer adapted to reject unauthorized data packets based on context information; and

providing filters adapted to reject unauthorized data packets based on rejection criteria from at least one of the context information and the policies.

7. (Original) The method of claim 1 further comprising updating the set of policies.

8. (Original) The method of claim 1 further comprising: detecting data packets from the regulated activities; and rejecting the data packets from the regulated activities.

9. (previously presented) An article comprising a computer-readable medium which stores computer-executable instructions for managing a network session, the instructions causing a computer to:

receive a set of policies from a server in a remote system, said remote system having predetermined configuration information;

allowing running of at least one application program in said remote system;

establish a secure virtual private network connection between the server and the remote system; and manage activities in the remote system based on both of the set of policies and a context of said at least one application program including at least a state of running of said at least one application program.

10. (Original) The article of claim 9, further comprising updating the set of policies.

11. (Original) The article of claim 9 wherein the instructions to reject the intervening processes comprises instructions to provide filters that are adapted to reject data packets based on rejection criteria.

12. (Original) The article of claim 11 wherein the rejection criteria includes predetermined static configuration information.

13. (Original) The article of claim 11 wherein the rejection criteria includes the set of policies.

14. (Original) The article of claim 9 wherein the instructions to reject the unauthorized activities comprises instructions to provide a session layer adapted to reject unauthorized data packets based on context user and application information.

15. (Original) The article of claim 9 wherein the instructions to reject the unauthorized activities comprises instructions to:

provide a session layer adapted to reject unauthorized data packets based on context information; and

provide filters adapted to reject unauthorized data packets based on rejection criteria from at least one of the context information and the policies.

16. (Original) The article of claim 9, further comprising instructions to:

detect unauthorized data packets from the unauthorized activities; and

reject the unauthorized data packets from the unauthorized activities.

17. (previously presented) A network system, comprising:

first and second devices, wherein the first device is adapted to:

deliver a set of policies to the second device;

and the second device is adapted to:

run an application;

use both said policies and a state of said application to detect data packets from unauthorized activities; and

reject data packets from the unauthorized activities.

18. (Original) The system of claim 17 further comprising a network stack.

19. (Original) The system of claim 18, wherein the network stack comprises:

a policy engine connected to the first device;

a policy store connected to the policy engine;

a socket interceptor connected to the policy engine; and

a packet guard connected to the policy engine.

20. (Original) The system of claim 17, the first device further comprising instructions to monitor the system for the intervening processes.

21. (previously presented) A network stack, comprising:

a policy engine;

a policy store adapted to interact with the policy engine and store a set of policies from the policy engine;

a socket interceptor coupled to the policy engine;

a packet guard coupled to the policy engine;

a configurable management process adapted to reconfigure the network stack and having instructions to:

receive policies in the policy engine from the policy server;

use the socket interceptor to detect and reject data packets from unauthorized users and applications and provide the packet guard with context information about the unauthorized users and applications including at least information about a running state of the application;

use the packet guard to filter unauthorized activities received from the network interface;

use the packet guard to filter the data packets from unauthorized users and applications based on the context information received by the socket interceptor; and

use the packet guard to filter data packets based on the policies.

22. (Original) The network stack of claim 21 further comprising a packet translator adapted to interact with the socket interceptor and the packet guard.

23. (Original) The network stack of claim 21 further comprising an interface to a network adapted to connect the network stack to the network, wherein the network has a policy server.

24. (Cancelled)

25. (Currently amended) The method as in claim 1, wherein said remote system includes a network stack, and wherein said regulating activities comprises reconfiguring the network stack to control filtering of network packets, based on said policies and said running state.

26. (previously presented) The method as in claim 1, wherein said policies include information about authorized kinds of information when certain applications are running, and said regulating activities comprises determining if a specified application is running, allowing a specified kind of network packet to pass only when said specified application is running,

and blocking said specified kind of network packet from passing when said specified application is not running.

27. (previously presented) The method as in claim 26, wherein said specified application is a word processing program, and said kind of network packet is word processing data.

28. (previously presented) The article as in claim 9, wherein said policies include information about authorized kinds of information when certain applications are running, and said manage activities comprises determining if a specified application is running, and allowing a specified kind of network packet to pass only when said specified application is running, based on said policies, and, blocking said specified kind of network packet from passing, when said specified application is not running, based on said policies.

29. (previously presented) A system as in claim 17, wherein said second device uses said policies to determine if an application is running and allows certain kinds of network packets, associated with said network application, to pass only when said application is running and to be blocked when said application is not running.

30. (New) A method, comprising:

establishing a virtual private network (VPN) session between a primary computing system and a remote computing system, wherein the primary computing system includes a security policy engine, and wherein the remote computing system includes a network stack;

transmitting information indicative of security parameters from the primary computing system to the remote computing system using the security policy engine;

configuring the network stack based on the information indicative of security parameters;

subsequently running a particular application program on the remote computing system;

selecting information indicative of updated security parameters based on a running state of the particular application program; and

dynamically reconfiguring the network stack based on the information indicative of the updated security parameters.

31. (New) The method of claim 30, wherein the primary computing system is a corporate local area network (LAN).

32. (New) The method of claim 30, wherein the remote primary computing system is a remote home network.

33. (New) The method of claim 30, wherein the particular application program is a word processing program, and wherein, when the running state of the word processing program indicates that the word processing program is not running, the information indicative of security parameters causes the remote computing system to block word processing packets received at the remote computing system.

34. (New) The method of claim 30, wherein the particular application program is a word processing program, and wherein, when the running state of the word processing program indicates that the word processing program is running, the information indicative of updated security parameters causes the remote computing system to not block word processing packets received at the remote computing system.